Security researchers outwit, bypass popular email encryption

May 14 2018

Germany's cybersecurity agency says German and Belgian researchers have found a way to outwit two widely used forms of email encryption.

IT security experts at the universities of Muenster, Bochum and Leuven were able to trick computers into covertly forwarding them the decrypted message.

Germany's Federal Office for Information Security said Monday that the method used exposes a "serious weakness" in the PGP and S/MIME encryption standards.

But it added that, correctly used and configured, both forms of encryption remain secure. To prevent a breach, users need to secure access to their mailboxes and prevent their email clients from loading HTML code from external websites.

The vulnerability was first reported by German newspaper Sueddeutsche Zeitung and public broadcaster NDR.

© 2018 The Associated Press. All rights reserved.